003 Certificate Maintenance

Issue: 11.0, 2013-sep-26

Authorisation: Martin Bergling, Technical Manager, CSEC
Table of Contents

1 Preface 3
  1.1 Purpose 3
  1.2 Typography 3

2 Introduction 5
  2.1 Overview 5
  2.2 Management of Confidential Information 5
  2.3 Management of the Certification Maintenance Process 6

3 Technical Concepts 7
  3.1 Assurance Continuity Purpose 7
  3.2 Terminology 7
  3.3 Assurance Continuity Paradigm 8

4 Characterisation of Changes 13
  4.1 Typical Minor Changes 13
  4.2 Typical Major Changes 14

5 Performing a Maintenance Impact Analysis 15
  5.1 Input 15
  5.2 Preliminary Work 15
  5.3 Steps in Performing the Maintenance Impact Analysis 15
  5.4 Output 17

6 Maintenance Impact Analysis Report (MIAR) 18
  6.1 Introduction 18
  6.2 Description of the Change(s) 19
  6.3 Affected Developer Evidence 19
  6.4 Description of the Developer Evidence Modifications 19
  6.5 Conclusions 19
  6.6 Annex: Updated Developer Evidence 20
1 Preface

This document is part of the description of the Swedish Common Criteria Evaluation and Certification Scheme ("the Scheme").

The Scheme has been established by the Swedish Certification Body for IT Security (CSEC) to evaluate and certify the trustworthiness of security features in IT products and the suitability of protection profiles (PP) to define implementation-independent sets of IT security requirements.

The objectives of the Scheme are to ensure that all evaluations are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and protection profiles; to improve the availability of evaluated IT products and protection profiles; and to continuously improve the efficiency and cost-effectiveness of the evaluation and certification process for IT products and protection profiles.

This document is part of a series of documents that provide a description of aspects of the Scheme and procedures applied under it. This document is of value to all participants under the Scheme, i.e., to anyone concerned with the development, procurement, or accreditation of IT systems for which security is a consideration, as well as those already involved in the Scheme, i.e., Scheme employees, evaluators, current customers, contractors, and security consultants.

The Scheme documents and further information can be obtained from the Swedish Certification Body for IT Security here:

Swedish Certification Body for IT Security
FMV / CSEC
Postal address: SE-115 88 Stockholm, Sweden
Visiting address: Banérgatan 62
Telephone: +46-8-782 4000 E-mail: csec@fmv.se
Web: www.csec.se

1.1 Purpose

The purpose of this document is to describe the procedures for assurance continuity within the Scheme and provides detailed information about the assurance continuity procedures and the responsibilities of each party involved.

General information about the Scheme is published in Scheme publication SP-001 Certification and Evaluation Scheme - Scheme Overview.

1.2 Typography

The following terms are used to specify requirements:

SHALL Within normative text, “SHALL” indicates “requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.” (ISO/IEC).

SHOULD Within normative text, “SHOULD” indicates “that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.” (ISO/IEC)

The CC interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.
Within normative text, “MAY” indicates “a course of action permissible within the limits of the document.” (ISO/IEC).

Within normative text, “CAN” indicates “statements of possibility and capability, whether material, physical or causal.” (ISO/IEC).
2 Introduction

This document defines an approach to assurance continuity that is in accordance with the procedures agreed for mutual recognition under CCRA. Assurance continuity provides the means to extend the validity of a Common Criteria certificate to an updated version of the certified product (more specifically the certified TOE) without having to perform a fully new certification.

Although the initiative to enter the assurance continuity process may come from a party distinct from the developer (i.e. a sponsor), it is expected that all preparations have to be done by the developer. As a consequence, all activities in this document are expressed as responsibilities of the developer rather than of a sponsor.

The first step in the assurance continuity process is to perform a maintenance impact analysis (MIA) to determine the implications of the changes to a certified product. If the impact is deemed minor, the certificate will be considered valid also for the changed version of the product. This is called (certificate) maintenance. Should the changes be deemed major, a re-evaluation will be necessary. During a re-evaluation only the parts of the evaluation affected by the changes have to be redone and a new certificate is issued for the changed product. A detailed description of re-evaluation procedures is given in the Scheme document SP-002 Evaluation and Certification.

The procedures for assurance continuity described in this document, are based on the CCRA document CCIMB-2004-02-009 Assurance Continuity: CCRA Requirements, Version 1.0.

2.1 Overview

The preface of this document outlines how the document fits into the context of the Scheme (Chapter 1). This introduction presents an overview of the assurance continuity procedures and the document itself (Chapter 2).

The following chapters present the Scheme procedures for assurance continuity:

- Description of technical concepts underpinning the assurance continuity paradigm including a description of the processes involved in both maintenance and re-evaluation (Chapter 3).
- Guidance on the characterisation of change (Chapter 4).
- Guidance on performing maintenance impact analysis (Chapter 5).
- Requirements for content and presentation of the maintenance impact analysis report (Chapter 6).
- All paragraphs are indexed to provide convenient referencing. Paragraph numbering is specific to the version of the document.

2.2 Management of Confidential Information

Documents received or drawn up by the Certification Body are official documents (“allmän handling”) and may be kept secret by the Certification Body only when it is required to protect the interests covered by articles in The Swedish Law on Publicity and Secrecy regarding:

- the security of the realm or its relationships with another state or international organisation
- inspection, control, or other supervisory activities of a public authority
- the prevention or prosecution of crime
- the economic interests of the public institutions
the protection of the personal or economic circumstances of private subjects

For further details on legal protection of confidential information, how to make the Certification Body aware of confidentiality claims and procedures for exchanging confidential information with the Certification Body please refer to SP-001 Certification and Evaluation Scheme - Scheme Overview.

2.3 Management of the Certification Maintenance Process

The start-up of the certification maintenance process is similar to a normal evaluation and certification process. The Sponsor or the ITSEF on behalf of the Sponsor SHALL submit to the Certification Body:

- an application for maintenance using Scheme publication SP-196 Certification Application with Terms - Form
- maintenance impact analysis report
- the certified security target
- the corresponding certification report
- developer test documentation
- if there are specific circumstances, an evaluator impartiality and independence justification

All the documents identified above are referred to as the maintenance application deliverables and SHALL be delivered with the application for maintenance. The application is considered complete when all the documents identified above have been delivered to the Certification Body in a finalised version or in a draft version that meets the requirements of the certification review process.
3 Technical Concepts

3.1 Assurance Continuity Purpose

The purpose of Assurance Continuity is to enable developers to provide assured products to the IT consumer community in a timely and efficient manner.

The awarding of a Common Criteria evaluation certificate signifies that all necessary evaluation work has been performed to convince the certification body that the TOE meets all the defined assurance requirements as grounds for confidence that an IT product or system meets its security objectives.

Assurance Continuity recognises that as changes are made to a certified TOE or its environment, evaluation work previously performed need not be repeated in all circumstances. Assurance Continuity therefore defines an approach to minimising redundancy in IT Security evaluation, allowing a determination to be made as to whether independent evaluator actions need to be re-performed.

3.2 Terminology

For clarity, the following terms are used in this paradigm description:

- the **certified TOE** refers to the version of the TOE that has been evaluated and for which a certificate has been issued;
- the **changed TOE** refers to a version that differs in some respect from the certified TOE; this could be, for example:
  - a new release of the TOE or of the product in which the TOE is a subset of functionality.
  - the certified TOE with patches applied to correct discovered bugs.
  - the same basic version of the certified TOE, but in a new operational environment (e.g. on a different hardware or software platform) as reflected in a new Security Target.
- the **maintained TOE** refers to a changed TOE that has undergone the main-tenance process and to which the certificate for the certified TOE also applies. This signifies that assurance gained in the certified TOE also applies to the maintained TOE.
- the **maintenance addendum** refers to one or more statements, regarding a specific certificate, in the Certified Products List (on the CSEC website) that the certificate has been extended to apply to the maintained TOE version.
- the **Maintenance Impact Analysis Report (MIAR)** refers to a report which records the analysis of the impact of changes to the certified TOE. The Maintenance Impact Analysis Report is generated by the developer who is requesting an addition to a maintenance addendum.
- the **Maintenance Report** refers to a publicly available report that describes all changes made to the certified TOE which have been accepted under the maintenance process. The Maintenance Report will be made available on the CSEC website.
- the **assurance baseline** refers to the culmination of activities performed by both the evaluator and developer resulting in a certified TOE, recorded or submitted as evidence and measurable by change to that evidence.
- the **developer evidence** refers to all items made available to the evaluators in support of an evaluation of a TOE.
- **Maintenance** refers to the process of recognising that a set of one or more changes made to a certified TOE have not adversely affected assurance in that TOE.
• **Re-evaluation** refers to the process of recognising that changes made to a certified TOE require independent evaluator activities to be performed in order to establish a new assurance baseline. Re-evaluation seeks to reuse results from a previous evaluation.

A product or system throughout its original evaluation is referred to as a TOE. Once the original evaluation is completed and a certificate awarded, it becomes the certified TOE. After a subsequent version of the certified TOE (changed TOE) has been added to the maintenance addendum, that version is considered to be a maintained TOE.

### 3.3 Assurance Continuity Paradigm

Assurance continuity seeks to exploit the fact that as changes are made to a certified TOE or its environment, evaluation work previously performed need not be repeated in all circumstances. The assurance continuity paradigm therefore defines the processes for maintenance and re-evaluation such that each seeks to recognise previous evaluation work.

Maintenance refers to the process undertaken by a developer and an ITSEF in order to have a unique TOE identifier change (e.g. version increment), resulting from a changed TOE, listed in the maintenance addendum for a previously issued certificate. It must be demonstrated that the changes to the TOE do not adversely affect the assurance baseline.

Re-evaluation refers to the evaluation of a changed TOE, such that the developer and the ITSEF could not (or chooses not to) demonstrate that changes to the certified TOE do not adversely affect the assurance baseline.

It is important to note that the maintenance process is not intended to provide assurance in regard to the resistance of the TOE to new vulnerabilities or attack methods discovered since the date of the initial certificate. Such assurance can only be gained through re-evaluation. Maintenance only considers the affect of TOE changes on the assurance baseline, it does not consider an evolving threat environment.

Figure 1 shows the primary paths through assurance continuity. Both the maintenance and re-evaluation processes have an equivalent starting point: when a change is made to the certified TOE [box 1]. This change might be a patch designed to correct a discovered flaw, an enhancement to a feature, the addition of a new feature, a clarification in the guidance documentation, or any other change to the certified TOE.
As a result of this change, a judgement needs to be made in regard to its resulting impact on assurance [box 2]. This includes an analysis of the developer evidence that would have to be updated to reflect the change, and regression testing of the code to be sure that it works when incorporated into the TOE. The basis for making this judgement is called maintenance impact analysis, which shall be performed by the evaluator, using developer evidence from the TOE developer, and recorded in a Maintenance Impact Analysis Report (MIAR); see Chapter 5 for more detail on the content of the Maintenance Impact Analysis Report. In doing this, further supporting documentation from the developer may be necessary.

CSEC reviews the Maintenance Impact Analysis Report to determine that it fulfils the requirements in chapter 6 regarding content and presentation, and that the conclusions regarding impact appear to be correct. It is required that the original certificate was issued by CSEC.
After accepting the Maintenance Impact Analysis Report, CSEC uses it to verify the evaluator's conclusions whether [box 3] each of the changes can be included under maintenance, or whether it has a major impact on assurance and is therefore considered sufficiently substantial that it requires re-evaluation.

If CSEC agrees that all changes are of minor impact, then [box 4] an maintenance addendum and a Maintenance Report, produced from the Maintenance Impact Analysis Report, are added to the Certified Product List on CSEC's web site. The Maintenance Report serves as an addendum to the certification report of the original certified TOE.

If CSEC finds that the change has a major impact, then the changed TOE must undergo re-evaluation in order for it to have an associated certification. This evaluation [box 5] makes maximum use of previously generated evaluation evidence, as well as the Maintenance Impact Analysis Report. Re-evaluation is described in detail in the Scheme document SP-002 Evaluation and Certification.

### 3.3.1 Maintenance

The purpose of Certificate Maintenance is to allow for minor changes (those that can be shown to have little or no affect on assurance) to be made to a certified TOE and have the resulting TOE version recognised as maintaining the same level of assurance as the certified TOE.

To achieve this aim, maintenance provides a mechanism which enables developers to report all changes to the TOE, to an evaluator which then has to analyse the affect of change and present their findings to a certification body (CSEC). This means that when a change occurs, developers has to document the changes to the same level of detail as is visible in the developer evidence and send information about the changes to an evaluator. The evaluator must do the analysis necessary to confirm that the assurance baseline has not been adversely affected. This process places an obligation on the developer to maintain all developer evidence (recording sufficient information in the Maintenance Impact Analysis Report about changes to documentary evidence would be considered maintaining that evidence), conduct and record appropriate testing. The evaluator shall confirm that previous analysis results have not been affected by changes to the TOE. Chapter 5: Performing an Impact Analysis further describes these types of activities. The maintenance process is described below.

**Process Description**

The maintenance process can be defined in terms of the necessary inputs, actions and outputs that lead to a new entry to the maintenance addendum for a Common Criteria certificate. The provisions of the certificate apply to all versions of the TOE that are listed in the maintenance addendum.

In order for CSEC to review the developer’s analysis, and in order to begin the process, the developer must formally apply for maintenance and deliver a Maintenance Impact Analysis Report and make all information about the changes available to CSEC. The cost associated with maintenance is specified in the Scheme document SP-008 Charges and Fees.

Once CSEC has received a formal application and a Maintenance Impact Analysis Report, CSEC will proceed with a review of the Maintenance Impact Analysis Report. There are two possible outcomes from the review:

- CSEC determines that the impact of changes on the TOE are considered major and the maintenance addendum will not be updated. Such changes would need to be considered during re-evaluation.
• CSEC determines that the impact of changes on the TOE are considered minor allowing that a maintenance addendum and a Maintenance Report may subsequently be added to the Certified Product List to show that the certificate also applies to the maintained TOE.

Once this determination is made, and after receiving the maintenance fee specified in SP-008 Charges and Fees, CSEC will inform the developer of the outcome. If the impact of changes is considered minor, a Maintenance Report and updated maintenance addendum is published on CSEC’s Certified Products List after receiving the maintenance fee specified in SP-008 Charges and Fees. The Maintenance Report is written by CSEC, and shall be approved by the developer before publishing. CSEC will protect the Maintenance Impact Analysis Report following the applicable procedures for evaluation evidence and in accordance with Swedish law.

In either case, major or minor, CSEC will record the underlying rationale for the decision in an (internal) Maintenance Impact Analysis Report Review Report, which will be used as a reference to maintain a consistent application of the maintenance procedures. In particular, it will be used as a source for reporting to the CCRA consistency process for maintenance.

**Maintenance Addendum**

The maintenance addendum serves as an addendum to the certificate for a certified TOE that lists the maintained TOEs derived from that certified TOE.

Each maintenance addendum will be published on the CSEC web site, as an extension to the entry for the original certificate in the Certified Product List. The information included in the addendum is as follows:

- Unique TOE identifier for each maintained TOE version, clearly related to that of the certified TOE.
- Reference to the Security Target associated with the maintained TOE. Note that if the only change to the Security Target is to the version of the TOE then the original Security Target may be referenced. If further changes are present, the Security Target shall be available from the CSEC web site.
- The Maintenance Report shall be referenced and available from the CSEC web site.

**Maintenance Report**

The Maintenance Report is considered to be an addendum to the Certification Report for the certified TOE. It provides details of all changes made to the certified TOE that have been accepted under the maintenance process.

The information contained in the Maintenance Report is essentially a subset of the Maintenance Impact Analysis Report content. The following sections should be included in the Maintenance Report:

- Introduction
- Description of changes
- Affected developer evidence

The content of each of these sections is described in Chapter 5 Impact Analysis Report. These sections may be sanitised when reproduced in the Maintenance Report by the removal or paraphrase of proprietary technical information if required.

The Maintenance Report should also contain a reference to the Certification Report for which it is an addendum.
3.3.2 Re-evaluation

When a change to a certified TOE has been determined to be of major impact, the implication is that a more concerted analysis, and by an independent evaluator, is required to assess the assurance of the changed TOE. A re-evaluation is performed in the context of an earlier evaluation, reusing any results from that earlier evaluation that still apply.

It is possible that the developer may opt directly for re-evaluation without ever creating a Maintenance Impact Analysis Report (for example, if the changes are so substantial that the changed TOE bears only a minimal resemblance to the evaluated TOE). Alternatively, even with substantial changes, the developer still may have contacted an evaluator to conduct a security impact analysis of the differences between the changed TOE and the evaluated TOE.

If a Maintenance Impact Analysis Report has been provided, this would be used as the basis for identifying those parts of the changed TOE remaining unchanged from the previously-evaluated TOE. As with all evaluations, analysis that has already been performed on parts of a TOE that remain unchanged need not be performed again, thereby maximising the amount of results of previous effort that can be re-used. To this end, the new evaluation reports are to a certain extent derived from the evaluation reports of the original TOE.

At the completion of the evaluation of the changed TOE, a CR is produced, along with a certificate for the changed TOE. This changed TOE becomes the updated basis for any future changes that might be made. The re-evaluation process is described in detail in the Scheme document SP-002 Evaluation and Certification.
4 Characterisation of Changes

The evaluator studies the changes described in the updated developer evidence and creates a Maintenance Impact Analysis Report based on that information. Next, the evaluator shall examine the changes in order to determine their impact upon the assurance of the certified TOE. A minor change is one whose impact is sufficiently minimal that it does not affect the assurance to the extent that the evaluator activities need be independently reapplied (although the developer is expected to have tested the changes as part of his standard regression testing). By contrast, a change deemed major has an impact that is substantial enough that it does affect the assurance and would consequently warrant independent re-application of the evaluator activities. Therefore, minor changes are addressed under maintenance, which is performed solely by the developer, while major changes are addressed under re-evaluation, which is performed by the evaluator.

It is important to note the difference between a change’s impact upon the certified TOE and a change’s impact upon the assurance of the certified TOE. A given change that is widespread and affects many parts of the TOE might have no effect upon the assurance of the TOE, or it could have far-reaching effects upon the assurance of the TOE. Similarly, a given change that affects only a very small part of the TOE might have no effect upon the assurance of the TOE, or it could have far-reaching effects upon the assurance of the TOE.

It is impossible to predict all possible changes to all possible TOEs and, therefore, to identify the impact of all possible changes (and whether a given possible change is minor or major). Consequently, there is no fixed method for identifying whether the security impact of a change is major or minor. The following offers a general guideline on the differences between major and minor changes, and also offers examples of exceptions.

4.1 Typical Minor Changes

Minor changes typically consist of changes to the TOE that have no effect on any claims about the TOE. Examples of minor changes that are therefore suitable to be addressed under maintenance are:

- Changes to the IT environment that do not change the certified TOE.
  For example, a change to the underlying hardware (where the hardware is not part of the TOE) or to software parts of the product that are outside the TOE boundary would likely be minor if the interface remains unchanged. However if the interface also changes, then it is likely a major change.

- Changes to the Certified TOE that do not affect the assurance evidence.
  For example, if a TOE has been certified to EAL1, a change to the source code and/or hardware schematics would not have an impact upon the assurance documentation. Nevertheless, the developer would have tested the changes as part of his standard regression testing.

- Editorial changes (grammatical, typographical, formatting) to any of the assurance evidence. For example, editorial changes to a functional specification that provide additional clarification would probably be minor. However, if a PP were to specify exact compliance as the degree of conformance, then even an editorial change to the ST’s security objectives statements or environment description would be major.

- Changes to non-executable text in the source code (such as comments) would typically be minor changes. But a change to compiler instructions would likely be a major change, as in cases when ALC_TAT is being claimed.
Changes to the development environment that have no notable effect upon assurance. For example, an update to the configuration management tool would be minor if the update did not affect the results of tracking the evolution of the TOE, or when ALC is not being claimed. However, if ALC is being claimed and an update to the configuration management tool produced entirely new results that would therefore have to be re-evaluated, then the change would be considered major.

Changes to the ST frontmatter. A change to the ST's identification or to the TOE identifier (e.g. product name change) would be minor. If any of the statements of Threats, OSPs, Assumptions, or Security Objectives change, without necessitating a change to the Security Requirements, these would likely be minor changes. If, however, any of the requirements statements do change, these would be major changes.

4.2 Typical Major Changes

Major changes typically consist of changes to the claims about the TOE and may (yet need not) result in changes to the TOE. Examples of major changes that are therefore suitable to be addressed under re-evaluation are:

- Changes to the set of claimed assurance requirements. This includes both changes to the families (for example, where ADV_TDS is the highest design abstraction claimed for the Certified TOE, and there is a desire to add a claim for ADV_INT) as well as a claim of a higher component within the same family. While the deletion of an assurance could arguably be considered a “minor” change, the result would require the production of a new certificate, which is done only under re-evaluation.

- Changes to the set of claimed functional requirements. This would likely change the TOE boundary, which would have to be re-assessed for correctness and soundness under re-evaluation.

- Use of procedures not assessed in the original evaluation. The use of new procedures that were not used in the original evaluation (such as delivery procedures different from those examined for ALC_DEL) would constitute a major change.

- A set of minor changes that together have a major impact upon the security. Although changes might be of minor impact in isolation, the collection of minor changes could have a major security impact. The combination of these would have to be re-evaluated.

It should be noted that a bug fix has no predictable extent of change to the certified TOE, nor a predictable effect upon the assurance of the certified TOE. Therefore, a “bug fix” might constitute either a major or minor change.
5 Performing a Maintenance Impact Analysis

5.1 Input
The following are inputs to the maintenance impact analysis process:
- developer evidence associated with the Certified TOE;
- change(s) description, which for example may be generated from life cycle quality processes and procedures.

5.2 Preliminary Work
Security categorisation of the TOE may be used as a tool to help assess if a change is within the scope of maintenance. For example, when a change is described in an impact analysis, the security categorisation may be consulted to identify the influence of the change on the developer evidence provided in the assurance baseline.

Security categorisation may include any security relevant development tools, secure delivery procedures, developer security procedures, development life-cycle activities, or the security relevant procedures affecting the use or administration of the configuration management system.

It should be noted that any additions to the TOE will need to be security categorised, according to the chosen approach, and any modified portions may need to have their security categorisation reviewed.

5.3 Steps in Performing the Maintenance Impact Analysis
During maintenance, it is the developer's responsibility to describe the changes made to the certified TOE. The developer shall also:
- contact an ITSEF
- ensure the availability of previous evaluation evidence

It is the evaluator’s responsibility to confirm that content and presentation verdicts for modified developer evidence can still be met. Having identified the affect of the change on the developer evidence, the evaluator is then able to conclude the security effect of the change.

Step 1 - Identify Certified TOE
The developer shall:
- determine the developer evidence provided for the certified TOE assurance baseline, including the certified TOE. All changes are applied against this baseline.

Step 2 - Identify and describe change(s)
The developer shall:
- describe the change(s) to the product with regard to the product associated with the certified TOE.
- Identify and describe the change(s) to the development environment with regard to the development environment of the certified TOE.

These changes are listed to the level of detail necessary to understand what was done, but not necessarily how it was done.
Step 3 - Determine impacted developer evidence

The objective of this step is to determine, considering each change from the previous step, which items of the developer evidence need to be updated. The developer should perform this work.

This step should be conducted in a systematic way, considering in turn each assurance component included in the assurance package for the certified TOE. The affect of the change on the assurance component and the evidence provided for that component. The following list can be used to facilitate such an approach.

For a change to the product, the following aspects should be considered:

- Has it affected the Security Target?
- Has it affected the reference for the TOE (if the assurance baseline includes a component from the ALC_CMS family)?
- Has it affected the list of configuration items for the TOE (if the assurance baseline includes a component from the ALC_CMS family)?
- Has it affected any of the TSF abstraction levels, that is, the functional specification, the high level design, the low level design or the implementation representation (if the assurance baseline includes a component from the ADV class)?
- Has it affected the architectural description (if the assurance baseline includes a component from the ADV_INT family)?
- Has it affected the TSP model (if the assurance baseline includes a component from the ADV_SPM family)?
- Has it affected the guidance documentation (if the assurance baseline includes a component from the AGD class)?
- Has it affected the testing documentation, that is, the analysis of test coverage, the analysis of the depth of testing or the test documentation (if the assurance baseline includes a component from the ATE class)?
- Has it affected the vulnerability analysis (if the assurance baseline includes a component from the AVA class)?

For a change to the development environment, the following aspects should be considered:

- Has it affected the Security Target?
- Has it affected the CM documentation (if the assurance baseline includes a component from the ALC class)?
- Has it affected the delivery procedures (if the assurance baseline includes a component from the ALC_DEL family)?
- Has it affected the procedures necessary for the secure installation, generation, and start-up of the TOE (if the assurance baseline includes a component from the AGD_PRE family)?
- Has it affected the developer security procedures (if the assurance baseline includes a component from the ALC_DVS family)?
- Has it affected the flaw remediation procedures (if the assurance baseline includes a component from the ALC_FLR family)?
- Has it affected the life cycle model (if the assurance baseline includes a component from the ALC_LCD family)?
- Has it affected the development tools (if the assurance baseline includes a component from the ALC_TAT family)?
The impacts on all the developer evidence should be considered, based on the change description, in order to check that all potential impacts have been identified. Note that the ST is likely to be affected, even if it is substantially similar to the original ST. If the TOE has changed, it would include at least a change to the TOE version number.

Previous versions of the Maintenance Impact Analysis Report may be used as input to this analysis.

For some developer action elements this determination may be simple (e.g. a new graphical user interface for the changed TOE, to be delivered in the same manner used for the TOE, will not have an adverse impact on ALC_DEL.1.1D), while for other requirements it may be more difficult (e.g. has the design for the user interface subsystem changed through the introduction of the new GUI and the affect on the material provided for ADV_TDS.1.1D).

The output of this step is a list of affected developer action elements.

Step 4 - Perform required modifications to developer evidence.

The objective of this step is to determine how should each of the affected developer evidence (identified during the previous step) be modified in order to address the corresponding content and presentation of evidence elements. The developer should perform this work.

It is sufficient to collect together changes required to developer evidence before actually implementing those changes.

Testing (regression testing) could be required to update the evidence. For instance, the developer may repeat a sample of the developer tests delivered for the evaluation. Regarding the Maintenance Impact Analysis Report, sufficient information about how the developer testing was updated would be required, commensurate with the testing components in the assurance baseline. If new tests were written to address a change, these are identified, with the test purpose, in the impact analysis report. However, the details of the test in terms of providing the test scripts including the individual test steps of the test, are not required.

If the change to the TSF is “invisible” at the lowest TSF abstraction available (e.g. the lowest level of TSF decomposition in the assurance baseline was the high-level design, and some source code is changed during maintenance, but the changes do not require modification to the high-level design), then the developer would show how the change was tested. The maintenance impact analysis report would then describe why this was considered to be adequate.

The output of this step is a list of updated evidence (this could take the form of a list of changes to the evidence - where, why, what).

Step 5 - Conclude

Determine the overall impact of the identified changes on the assurance of the certified TOE. Conclude: minor or major impact. The evaluator shall perform this work.

See Chapter 4 for a discussion on the characterisation of change.

5.4 Output

- Maintenance Impact Analysis Report (MIAR);
- Updated developer evidence.
6 Maintenance Impact Analysis Report (MIAR)

This chapter describes the minimum content of the Maintenance Impact Analysis Report. The contents are portrayed in Figure 2; this figure may be used as a guide when constructing the structural outline of the document. The Maintenance Impact Analysis Report is a required input for the maintenance process.

![Maintenance Impact Analysis Report](image)

Figure 2 - Maintenance Impact Analysis Report information content

6.1 Introduction

The developer shall report the Maintenance Impact Analysis Report configuration control identifiers.

The Maintenance Impact Analysis Report configuration control identifiers contain information that identifies the Maintenance Impact Analysis Report (e.g. name, date and version number).

The developer shall report the current TOE configuration control identifiers.
The TOE configuration control identifiers identify the current version of the TOE that reflects changes to the certified TOE.

The developer shall report the configuration control identifiers for the CR, and the certified TOE.

These configuration control identifiers are required to identify the assurance baseline and its associated documentation as well as any other changes that may have been made to this baseline.

The developer shall report the configuration control identifiers for the version of the ST related to the certified TOE.

The developer shall report the identity of the developer.

The identity of the TOE developer is required to identify the party responsible for producing the TOE, performing the impact analysis and updating the evidence.

The developer may include information in relation to legal or statutory aspects, for example related to the confidentiality of the document.

6.2 Description of the Change(s)

The developer shall report the changes to the product.

The identified changes are with regard to the product associated with the certified TOE.

The developer shall report the changes to the development environment.

The identified changes are with regard to the development environment of the certified TOE.

6.3 Affected Developer Evidence

For each change, the developer shall report the list of affected items of the developer evidence.

For each change to the product associated with the certified TOE or to the development environment of the certified TOE, any item of the developer evidence that need to be modified in order to address the developer action elements shall be identified.

6.4 Description of the Developer Evidence Modifications

The developer shall describe briefly the required modifications to the affected items of the developer evidence.

For each affected item of the developer evidence, the modifications required to address the corresponding content and presentation of evidence elements shall be briefly described.

6.5 Conclusions

For each change the evaluator shall report if the impact on assurance is considered minor or major.

For each change the evaluator should provide a supporting rationale for the reported impact.

The evaluator shall report if the overall impact is considered minor or major.

The evaluator should include a supporting rationale, taking the culmination of changes into consideration.
6.6  

**Annex: Updated Developer Evidence**

The developer *shall report* for each updated item of developer evidence the following information:

- the title;
- the unique reference (e.g. issue date and version number).

*Only those items of evidence that are notably changed need to be listed; if the only update to an item of evidence is to reflect the new identification of the TOE, then it does not need to be included.*